California Enterprise Architecture Program

Technical Architecture Framework (TAF) 1.0

August 31, 2006

Revision History

Release	*Description*	*Date*
1.0	***Initial Publication***	***08/31/06***

Table of Contents

Credits and Disclaimers

Appreciation for the work accomplished and acknowledgement for the framework and portions of the information must be credited to The Technical Reference Model (TRM) Version 1.1 produced by the Federal Enterprise Architecture Program Management Office (FEAPMO) and the enterprise architecture framework developed by the National Association of State CIO's (NASCIO). Many of the terms and their definitions were taken directly from these sources; other information was inserted or changed to reflect the design and requirements for the State of California. Likewise, California's Technical Architecture Framework also used information from Gartner's Enterprise Architecture (EA) Framework and several states who were already implementing EA programs. These states include Michigan, Virginia, Washington, South Carolina, North Carolina, Pennsylvania, and New Mexico.

1.0 Overview

The Technical Architecture Framework (TAF) was developed by the California Enterprise Architecture Program (CEAP) under the auspices of the State CIO, IT Council, and Enterprise Architecture & Standards Committee. This document extends the State's Enterprise Architecture Framework by defining a common approach for organizing, integrating, and managing technology across or within organizational boundaries. The TAF is intended to be applicable to all offices of the Executive Branch and maybe adopted by other Governmental Agencies including local government.

The TAF provides a common framework conveyed by the Technical Reference Model (TRM) that organizes and describes technology and furnishes the approach by which the State's Enterprise Technical Architecture (ETA) (including technology standards) is created and maintained. This approach calls for the EA Committee to establish state-level domain teams who are given the responsibility for assessing and developing technology standards for each technology domain identified by the TAF and the TRM. Domain teams use the Domain Team Handbook that provides the processes and templates needed to create domain specific architecture reports and state level domain architectures. The domain architecture report identifies business and technology drivers, IT principles, best practices, general technical direction, migration approaches, and recommends broad technology standards. The domain architectures are documented using the templates included in the domain team handbook and provide specific technology standards and technical direction. More importantly, these standards articulate both the "As Is" and "To Be" state of technology and provide technical guidance on when and how product component technologies and industry standards may be used. The aggregation of domain architecture reports and domain architectures (templates) constitutes California's ETA which is monitored and maintained by the domain teams and CEAP.

State-level technical standards are a key source of information needed to help define solutions for strategic initiatives. The Strategic Initiative to Service Delivery process (Figure 1) shows how architecture products are used to help identify the project's technical requirements and/or select the most appropriate technologies for use in provisioning the business solution. The project's proposed solution attempts to appropriately leverage both business activities and the use of technology across (or within) organizational boundaries from a state-wide perspective.

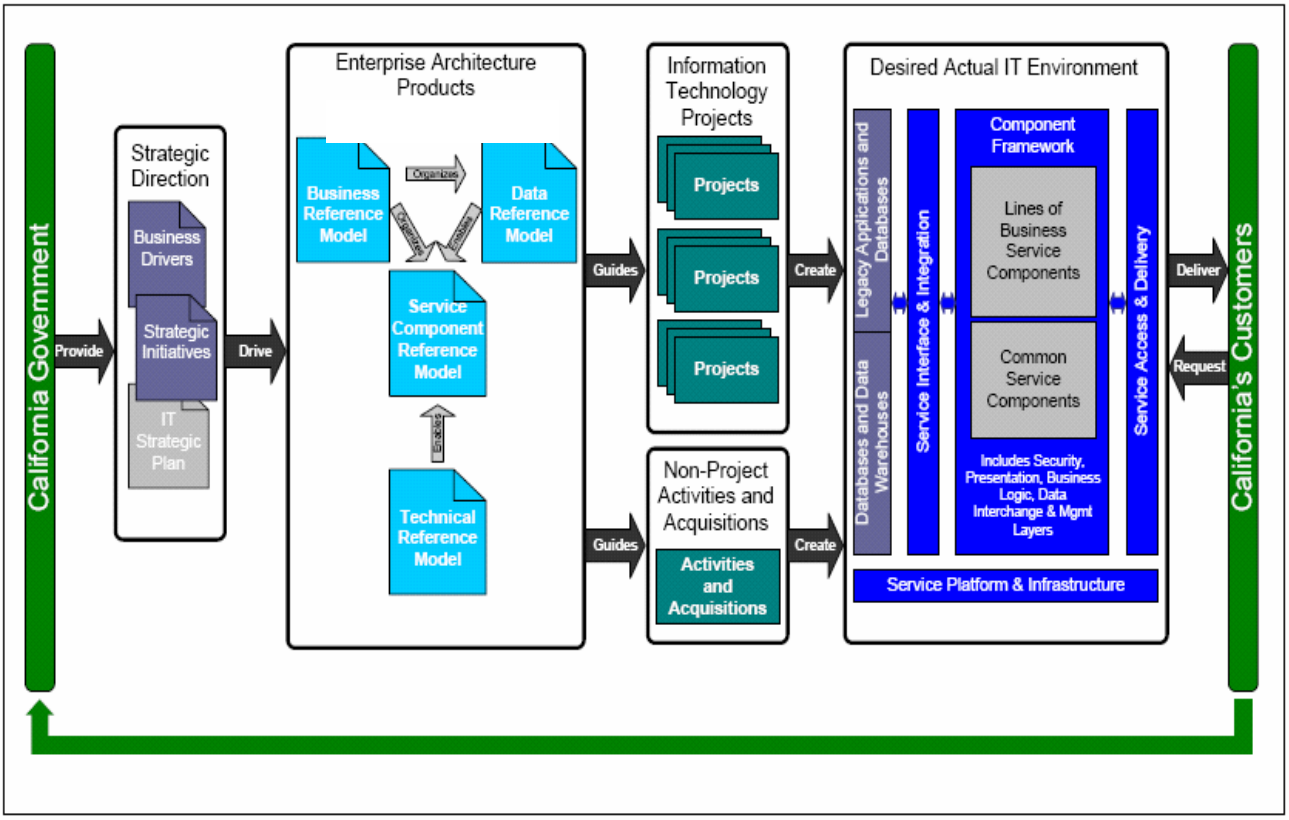

Figure 1- From Strategic Initiative to Service Delivery Model

Implementing the TAF to create an ETA that provides technical direction and technology standards supports IT investment decision making processes. The technical standards, which are produced from using the framework, provide program and project managers with the viable technology options from which to select their enabling technologies. The ETA standards indicate when and how technology components may be used based on lifecycle stage and product supportability. Adhering to the guidance contained in the ETA helps minimize technological risk and improve the return on investment (ROI) for supported business activities or identified project initiatives. This information also allows program managers and CIO's to determine when technology upgrades are required and how they can be leveraged across the State's or within the enterprise's IT investment portfolio.

2.0 The Technical Architecture

2.1 Context

The State's IT Strategic Plan seeks to lower costs and improve the security, reliability, and performance of the State's IT Infrastructure, and calls for adopting a statewide Enterprise Architecture (EA) to achieve these desired outcomes. California's EA Framework - Release 1.0[1] establishes the conceptual framework and the four architectural views (Figure 2) needed for identifying and developing business solutions and service delivery strategies within state government. However, the overall EA Framework must be extended to become useable. Each architectural view requires development of a supporting framework and reference model that organizes and provides the information required to help ensure that each business solution is functionally aligned and leveraged across the State as the enterprise.

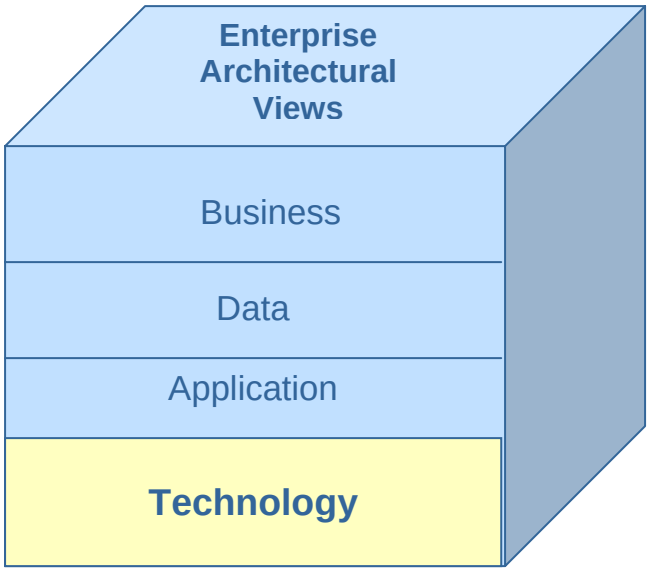

Figure 2 - California Enterprise Architecture Framework

[1] http://www.cio.ca.gov/ITCouncil/Committees/PDFs/California_EA_Framework_Final.pdf

The technology architecture exists to enable business system solutions. This architectural view uses a technical reference model to organize technology and provides the technical standards needed to create a leveraged IT Infrastructure on which the enterprise's applications run and business services are provided. Technology considered for use by the infrastructure must be evaluated, organized, and assembled from an enterprise perspective in order to maximize functional and economic value. The Technical Architecture uses the EA's core principles[2] to guide the development of its supporting framework and the resultant ETA. Business and other drivers cause technical evaluation to focus on e-Government service delivery, secure information sharing, seamless integration, operational performance, and how best to leverage existing or planned IT investments. The Technical Architecture is where the linkages between business system solutions and planned use of technology become real.

2.2 Technical Architecture Framework Goals

The following goals are established for the Technical Architecture Framework:

- Provide a common language, approach, and process needed to guide selection and use of information technology within the State.
- Establish a framework that can be used to develop and maintain California's Enterprise Technical Architecture and related technology standards.
- Furnish the information needed to facilitate development of leveraged technology solutions in support of business system initiatives.
- Provide technology direction and standards to help guide Agency and Department technology choices and requirements specified in FSR's, RFI's, RFP's, and other development efforts.
- Establish a technology standards exception and change control review process.
- Help consolidate technology solutions and lower the total cost of operations and maintenance of the State's IT infrastructure.

2.3 Technical Architecture Principles

The California's Enterprise Architecture Program specifies the core principles[2] that guide development of the Technical Architecture Framework's concepts and approaches. In addition to these core principles, the following principles are provided for the technology architectural view.

2.3.1 Technology Perspective

Technology is not a separate discipline or an end unto itself, but must be properly aligned with business services.

Rationale:

Technology supports the overall mission of government by providing the tools needed to increase convenience, capacity, and effectiveness of the business services provided to citizens and business partners.

Implications:

- Strategic business plans and programs drive technology.

[2] http://www.cio.ca.gov/ITCouncil/Committees/PDFs/CEAP_principles_FINAL.pdf

- Business owns the services and the delivery system.
- There are no "technology projects", but there are business initiatives.
- Technology is an enabler and component of "business" initiatives and projects.
- Technology provides the maximum leverage when business processes are re-engineered prior to automating.

2.3.2 Technical Complexity

Choose technologies that reduce the level of hardware or software complexity included within the Enterprise Technical Architecture.

Rationale:

Reducing technological complexity decreases total cost of ownership associated with providing an enterprise IT infrastructure and expedites system development activities.

Implications:

- Reduces application integration effort
- Decreases the number of vendors, products, and configurations needed for the enterprise's IT infrastructure environment
- Expedites software development and maintenance because fewer tasks are required.
- May require some performance and functionality trade-offs
- Provides agility for adapting and responding to change.
- Requires organizations constrain the number of permutations in products to limit support costs.

2.3.3 Evergreening the ETA

Conducting periodic reviews of the technology domains ensures relevance and agility of the ETA.

Rationale:

The ETA must be maintained to preserve its usefulness and value to the enterprise.

Implications:

- ETA domains must be periodically reviewed and modified to maintain relevance and establish planned technology evolution.
- Requires establishment of an inclusive, ongoing, and decisive technical architecture review and change control process.
- Necessitates specific triggers that impact the ETA be established and monitored.
- Prevents the technical architecture from losing its value if not maintained.
- Ensures agility and responsiveness in meeting new business needs or service requirements.

2.4 Technical Architecture Framework

As a component of California's EA Program (CEAP), the Technical Architecture Framework (TAF) (Figure 3) provides a common, disciplined approach for creating Enterprise Technical Architectures (ETA) and technology standards. The TAF document identifies the state's technical reference model (TRM) structure, technology domains, and specifies approaches for implementing the framework and managing the resultant

ETA. Appendix 1 - Domain Technical Reference Models uses the TRM's hierarchical structure to establish domain specific TRMs and provides a detailed description of the disciplines and technology areas within each domain. The Domain Team Handbook describes the role of a domain team and provides both processes and templates needed to create and maintain domain level architectures. Collectively, these domain architectures convey California's ETA and provide the technology direction and standards needed to help leverage development of state-level shared services and Agency/Department level initiatives.

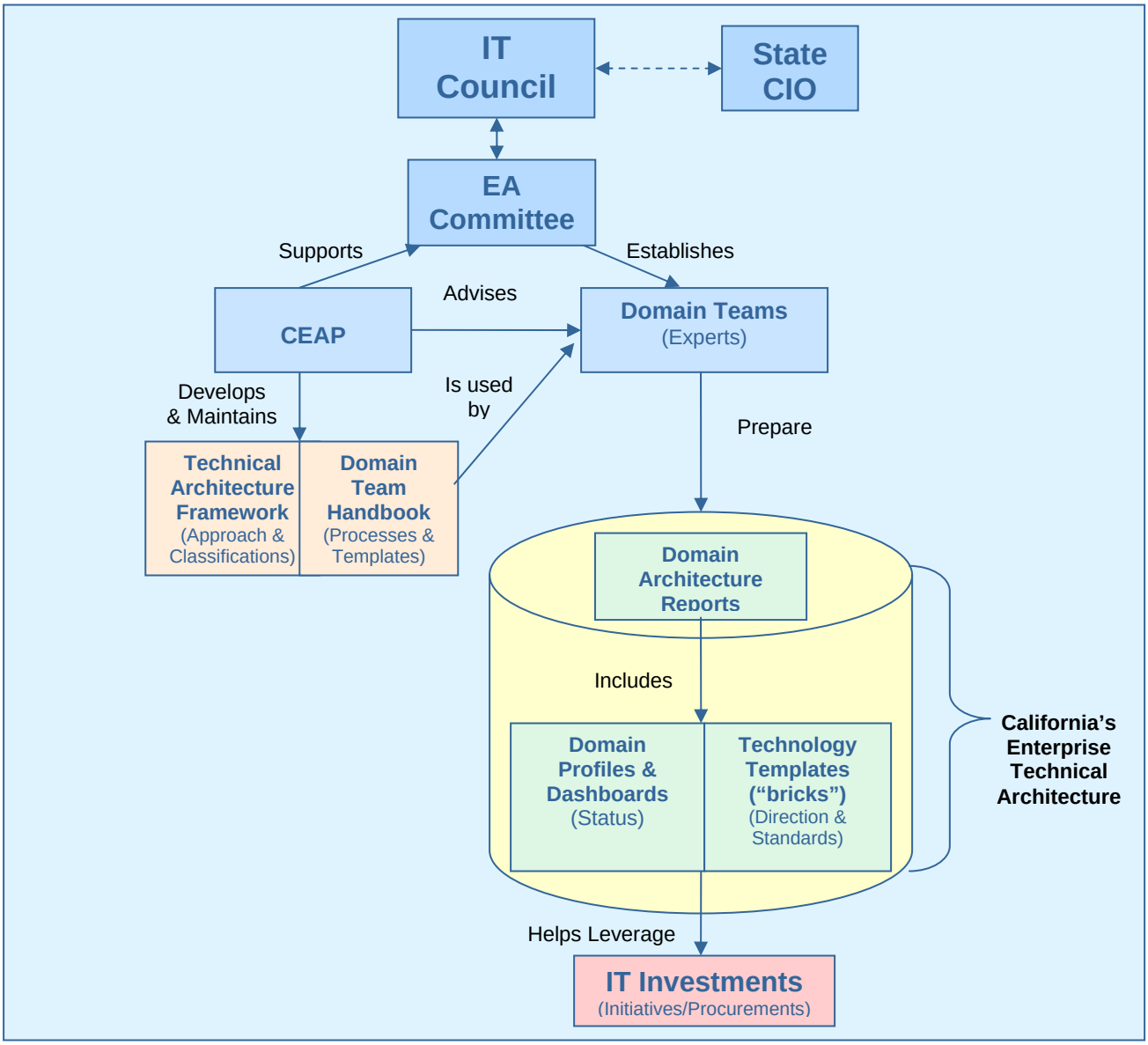

Figure 3 – Technical Architecture Framework Overview

3.0 The Technical Reference Model (TRM)

A Technical Reference Model (TRM) is used to organize, categorize, and describe the technologies used within the State. California's TRM is based on a combination of the information obtained from the National Association of State CIO's (NASCIO) Enterprise Architecture Development Tool-Kit v3.0, the Federal Enterprise Architecture Program (FEAP), Gartner's EA Framework, and a review of other State's Technical Architecture Programs.

The TRM employs a hierarchal structure consisting of four levels (Figure 4) that classify and relate technology information. These four levels successively narrow the focus of the technology included within a domain until a specific technology product or standard is identified. Figure 5 (page 13) provides a sample representation of the TRM hierarchy for a portion of the Application Domain and shows the relationship among the different levels. This TRM structure complies in principle with both NASCIO and Federal Enterprise Architecture Program technical reference models.

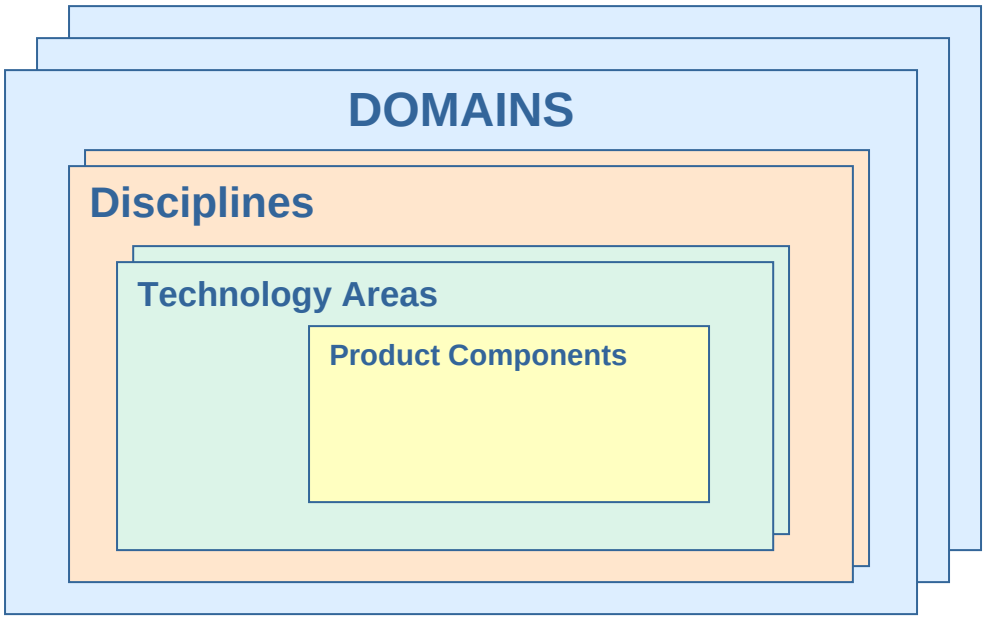

Figure 4 - California's Technical Reference Model (adapted from NASCIO)

Domains – The highest level of the Technical Architecture and forms the main building blocks of the Enterprise Technical Architecture. California's Technical Reference Model has seven domains that cover the totality of technology standards applicable to state government. The domain structure and associated descriptions are listed in Section 4.2.

Disciplines – Logical, functional subset of the domain and are a cohesive unit with regard to its subject areas and stakeholders. Disciplines allow further breakdown of a domain into manageable pieces. For example, the Application Domain consists of several Technology Disciplines (e.g. Access Channel, Presentation, Web Server, Business Components, Software Engineering, etc.). Each discipline is normally comprised of multiple technology areas.

Technology Areas – Are technical topics that support functional areas within a discipline. The Access Channel discipline for example consists of multiple Technology Areas (e.g., Windows, Web Browsers, Wireless/PDA's, etc.). Each technology area can have specific products, protocols, or configurations associated with it and therefore contain multiple Technology Elements.

Product Components – Are specific technology elements or products within a technology area and include protocols, products, configurations, and standards. Product Components finalize the details of the TRM and defines the lowest level at which technology is managed.

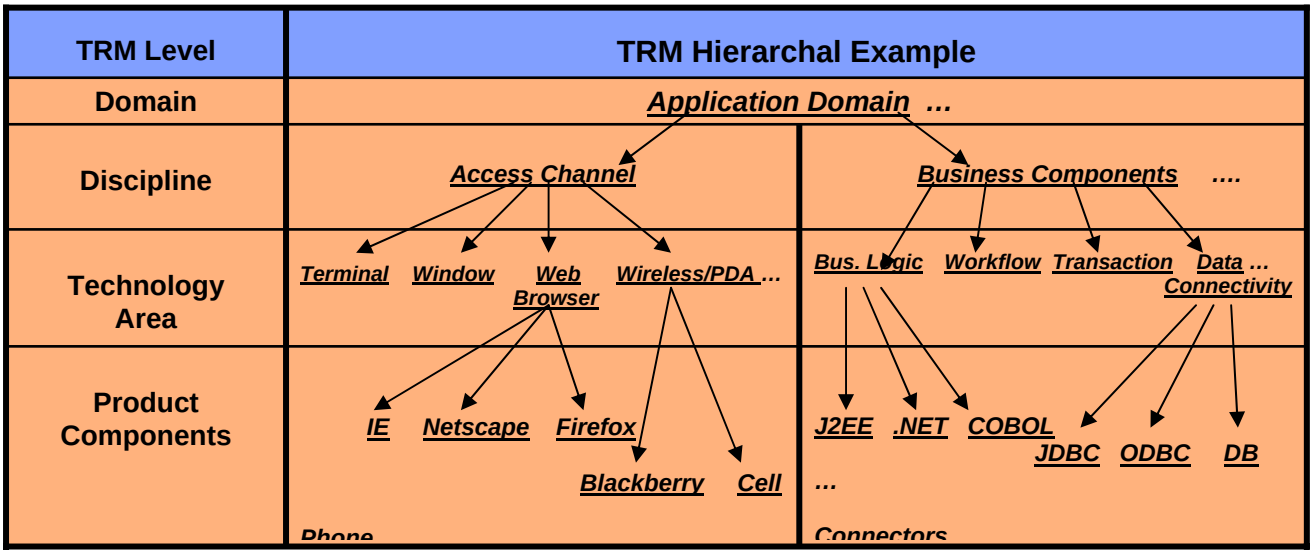

Figure 5 – TRM Levels of Detail for the Application Domain

4.0 Enterprise Technical Architecture (ETA) Domains

California established seven domains around which all technology information and standards are organized. These domains are depicted below (figure 6). This section provides a general description of each technology domain. The TRM hierarchy is used to establish technology groupings contained within each of these domains. Domain specific TRMs are provided at Appendix 1. These TRMs classify and describe technology groupings within each domain down to the technology area.

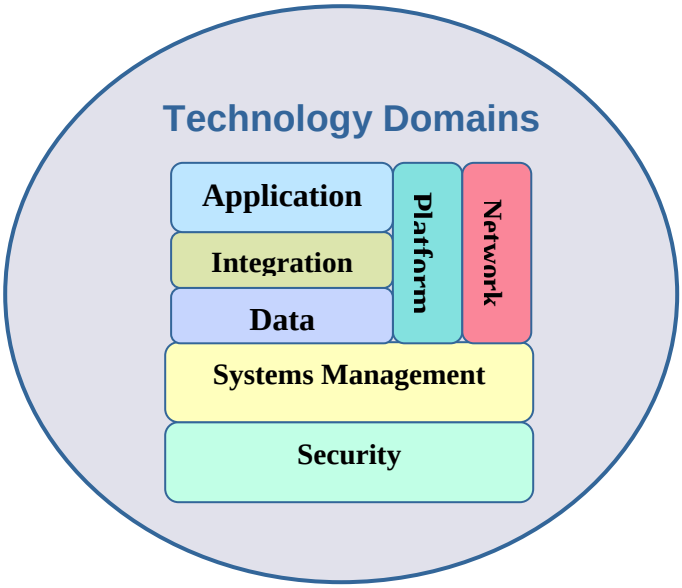

Figure 6 - California's Technology Domains

Domain teams will use the domain descriptions and TRM information contained in Appendix 1as the foundation for developing an architecture for their domain. The domain architecture identifies both the product components and technical standards contained therein. Technologies from these domain architectures are assembled to provide a leveraged, operational IT infrastructure on which all business services and applications systems run.

4.1 Application Domain

The Application Domain defines the technologies needed to develop an application (or service) and provide it for use. These technologies provision both the development and production environments. This domain provides the access channels needed for the interface between an application and its users, and the means by which information and data is presented or received. The capabilities needed to implement business functionality in terms of business logic, business rules, workflow, process flow, transactions, batch jobs, and accessing data stores is also included.

The Application Domain furnishes a complete set of software engineering capabilities needed to support both development and maintenance activities. This includes the tools for modeling business activities,

maintaining an integrated development environment, implementing software configuration through all stages of the software development lifecycle, and managing test activities. Test management tools support the development of test plans needed during various phases of application development and delivery. These tools not only help document testing, but also manage test results.

Additionally, process control tools are included in this domain. These tools support the processes needed to manage both individual projects and the collective set of the applications and IT services being maintained by the enterprise. Project management tools guide and document individual project activities from initiation and planning phases through development and delivery. Portfolio management tools provide capabilities to collectively manage a portfolio of delivered applications currently being maintained and operated by the enterprise.

Finally, this domain includes the technologies that deliver shared applications and services that are jointly developed and/or used by two or more agencies/departments. These applications are often provisioned by using Commercial-Off-the-Shelf (COTS) software packages (e.g. ERPs, CRMs, Portals, etc.) that have been adapted and implemented using a bundled set of technologies. Even though these bundles include technologies from several domains, they are managed as a single product component (e.g. ERP - SAP Websphere) Shared services are web services that have been built and delivered for use across the enterprise (e.g. a Payment Service or an Identity Service). These shared services may be built by a vendor or a federal, state, or local governmental entity.

4.2 Data *Domain*

The Data Domain provides the technologies used to manage all data/information created and maintained by the enterprise. Technology in this domain implements data management functions for defining data and conceptualizes the way in which people perceive and use it. Database technologies furnish the modeling capabilities needed to logically organize, structure, and define data in preparation for implementation as an operational data store. These technologies also provide the database management systems (DBMS's) to physically implement the logical data model so that it organizes and collects information in such a way that computer programs can quickly select desired pieces of data for use in support of business workflows. Utility tools included in this domain help preserve data continuity through the use of automated data base backup and restoral capabilities.

This domain furnishes a specialized set of decision support related technologies to create a data warehouse from operational data stores and processes it into useful information about the enterprise's business condition. This technology along with others (e.g. Data Analytics, ETL, OLAP, BI, and reporting) support management's need to analyze operational data, generate management reports, provide rapid response to answer business questions via complex, analytical (or ad hoc) queries, and to make strategic business decisions .

A highly specialized group of database technologies is used to organize, manage storage for, provide efficient retrieval of, and present geospatial information (e.g. imaging, mapping, hydrology, etc.).

4.3 Integration Domain

The Integration Domain specifies how various systems, operating on different platforms and/or in external environments, can effectively work together to seamlessly interact and exchange data over various communication systems. This domain allows an enterprise to interoperate internally and externally through the use technologies that provision the necessary interfaces and interoperability.

Interface technologies provide the capabilities needed for communicating, transporting, and exchanging information across networks (LAN and WAN) to complete transactions using a predetermined framework. All interface technologies implement the communications boundary between two entities (e.g. computer programs, applications) which allows for the exchange of information between them. Major interface technologies include Service Discovery, Service Description, Middleware, and Legacy.

Service Discovery provides the wherewithal to locate web services (i.e. UDDI) or Application Program Interfaces (API's). Service Description technology defines each service (i.e. WSDL) and how it can be used and allows implementation of the method by which applications, systems, or web services are registered and discovered for use. API technology enables the interface that a computer system, library or application in order to allow requests for service.

Middleware technologies increase the flexibility, interoperability, and portability of the existing infrastructure by linking or "gluing" separate applications together in support of business workflows. Several middleware technologies are used to control the communication over the web between a client and an object on a server (e.g. RPC, MOM, transaction managers, Enterprise Service Bus, etc.). The Enterprise Service Bus (ESB) is a significant new technology within this group because it provides a "universal" set of connections to link numerous independent systems together. This is especially useful for enabling service oriented architecture.

Legacy interface technologies furnish integration for programs that exist within the mainframe environment. These interfaces are based on a terminal to mainframe connection that implements communications to support either transactional or batch based processing. Application outside the mainframe environment can interface with mainframe applications though a special set of middleware based primarily on messaging.

Interoperability technologies provide capabilities for discovering and sharing data across disparate systems and vendor platforms. These technologies format and classify data, provide standards for sharing information/data (i.e. XML), and transforms data for use in an application or within a graphical user interface.

Data Format/Classification defines the structure of a file and the formats for data in that file (e.g. database, word processing, graphics, executable program, etc.). Each format defines its own layout of the data.. EXtensible Markup Language (XML) provides a standard format for web data and is also being used as a common data format at all levels of the architecture. Data Transformation technologies allow data to be exchanged (via transformation) between systems that are using different XML schemas.

4.4 Platform Domain

The Platform Domain establishes the underlying hardware and software environment needed to furnish the processing environment to support business system processing and development activities. Technologies in this domain include Hardware Platforms, Functional Servers, Supporting Platforms, Peripherals, and Storage Systems. Collectively these technologies provide the computer platforms needed by the business user, the network, the mainframe, the development environment, peripherals, and storage systems required to establishing and supporting the various processing environments.

Hardware Platform technology furnishes the various types of programmable machines which are capable of responding to sets of instructions and executing programs. This includes all computer platforms from the mainframe down to personal computer devices and their operating systems. These technologies also include the means to create virtual platforms that divide a single hardware platform into multiple logical areas in which separate and distinct processing occurs.

Functional Servers are computers or devices on a network that manage network resources and share an application for multiple users (e.g. web server, mail server, application server, file server, database server, etc.). These server technologies include the hardware, operating system, server software, and networking protocols to provision the functions they support.

Supporting Platforms provide the underlying hardware and software for a system which defines a standard ((e.g. J2EE, .Net, wireless, etc.) around which an application or system can be developed. These platforms provide processing support for both development and production environments required for running the resultant application's programs. Special supporting platforms are needed to provision applications that utilize wireless or portal technologies.

Peripherals furnish computer devices that are not part of the essential computer or network. Typically these technologies focus on input or output hardware (e.g. printers, scanners, readers, faxes, etc.) They can be external or internal and can be for a PC, workstation, or network. Storage System platforms are designed to provide shared storage access across a network (e.g. SAN, NAS, tape, etc.)

4.5 Network Domain

The Network Domain provides a communications infrastructure for achieving connectivity between two physically separate systems. Computers and devices are joined together by a physical communications link allowing information to be passed on demand between the requestor and recipient. This domain defines the various technologies required to enable this connectivity and securely exchange information. It does not include user workstations, server platforms or their operating systems. The Network Domain technologies include those required to implement Internet/Extranets, Intranets, Wireless (networks), Network Appliances, and Network Services.

Internet/Extranet technologies connect networks to other networks globally forming an overall network in which any computer can communicate with any other computer as long as they are both connected to the Internet. Extranet technologies are used to establish networks that are only partially accessible to selected entities on the internet. Access is provided for various levels of accessibility to outsiders based on network security.

Intranet technologies are similar to an internet/extranet technologies (e.g. network based on TCP/IP protocols), but they are used to create a network for the exclusive use of an organization. The capabilities associated with intranets insure that the organization's network is only accessible only to the organization's employees or others authorized users. An intranet's Web sites look and act just like any other Web sites, but there is a firewall that fends off unauthorized access.

Wireless network technologies utilize radio media (e.g. radio, spread spectrum, cellular technology, satellites, and microwave) rather than by wires to establish connectivity. These technologies can handle voice, data, video, and images, and they allow wireless networks to be interconnected with regular computer networks.

Network Appliances include specialized devices used to control access to and/or pass data between networks (i.e. routers, gateways, firewalls, and proxy type servers). Network services provide special network functions that allow access or connectivity to network resources or devices (e.g. directory services, DNS, and DHCP) and help manage the operational aspects of the network including security (e.g. network alerts encryption, IP security, and spam blocking.)

4.6 Systems Management Domain

The Systems Management Domain identifies the technology components needed to monitor and control IT services and the supporting infrastructure. Systems management technology enables the functions associated with IT Service management specifically service support and service delivery. Technologies in this domain help implement IT Infrastructure Library (ITIL) concepts to insure adequately managed IT services are available to the user and that the performance of IT infrastructure meets current and projected service delivery requirements.

Service Support technologies focus on ensuring user access to the appropriate services needed to carry out their business functions and supporting the users who are having difficulties with or are requesting a change to an IT service (i.e. service desk and the areas of incident, problem, change, configuration, and release management). Service Delivery technologies allow management of the technical infrastructure including the technology lifecycles of its component parts to help sustain current service performance levels and address future needs for the business as a whole. Key functions supported by this technology include service, capacity, availability, IT financial (e.g. IT assets), continuity, and security management.

4.7 Security Domain

The Security Domain identifies the set of components needed to protect the State's information assets in compliance within legal requirements for confidentiality and integrity while enabling public access to appropriate information. This domain establishes criteria, specifies techniques associated with information security, and identifies key security mechanisms that provide identification, authentication, administration, and audit services. Using these mechanisms insures data confidentially, availability, and integrity are maintained while performing business services. Key security areas include security administration and management, identity management, privacy, and web services security.

Administration & Management technologies furnish the capabilities for insuring that information stored on a computer or network cannot be accessed or compromised by any individuals without proper authorization. These technologies enable access policy implementation, security monitoring and alerts, virus protection, compliance auditing, forensic analysis, data encryption, and electronic signatures. These technologies afford the capability to log important activities that occur during the operation of the enterprise; track activity by user concerning what, where, and when data was accessed for critical applications; and provide audits for both disaster recovery purposes as well as investigations of misuse.

Identity Management technologies allow management the unique names of persons, devices, or the combination of both that is recognized by a system. These technologies furnish authentication, authorization, and accounting services based on receipt of valid identity data to ensure the security of networks and other computer resources.

Privacy technologies provides the capability for an individual or group to keep their lives and personal affairs out of public view, or to control the flow of information about themselves as directed by legal mandates or user preferences. Supported functions include compliance management policy, profiling, and personalization.

Web Services Security technologies provide frameworks and standards for implementing secure access to and proper handling of data passed across the Internet and other networks (e.g. WS*). These technologies insure message integrity and confidentiality.

5.0 TAF Implementation

5.1 ETA Development Approach

The TAF is used as the basis for development of the State's ETA and technology standards. The State EA Committee charters Domain Teams to develop and maintain domain architectures. Each Domain Team uses the TAF framework and the architecture development process (provided in the Domain Team Handbook) to create a portion of the State's ETA. Domain Teams produce a set of deliverables (Figure 7) which identify the technologies, the technical direction, and technology standards pertaining to their domain. Domain Architecture Reports (DAR) document the results of the ETA development process by providing a domain assessment and recommending technology standards. Domain teams also establish domain architectures and update the domain TRM in Appendix 1 of the TAF as needed. State level domain architectures normally consist of a Domain Profile (a synopsis of the DAR) and a domain dashboard depicting the domain architecture status and technology direction. Domain teams may also elect to create "bricks" to convey specific technology standards or indicate a migration path. California's Enterprise Technical Architecture (ETA) is populated as each domain report and domain architecture is reviewed and published for use. State level domain architectures provide the general standards and overall technical direction needed to facilitate consolidation of the State's technology base. CEAP provides advice and assistance to Domain Teams and acts as liaison between the Domain Team and the EA Committee.

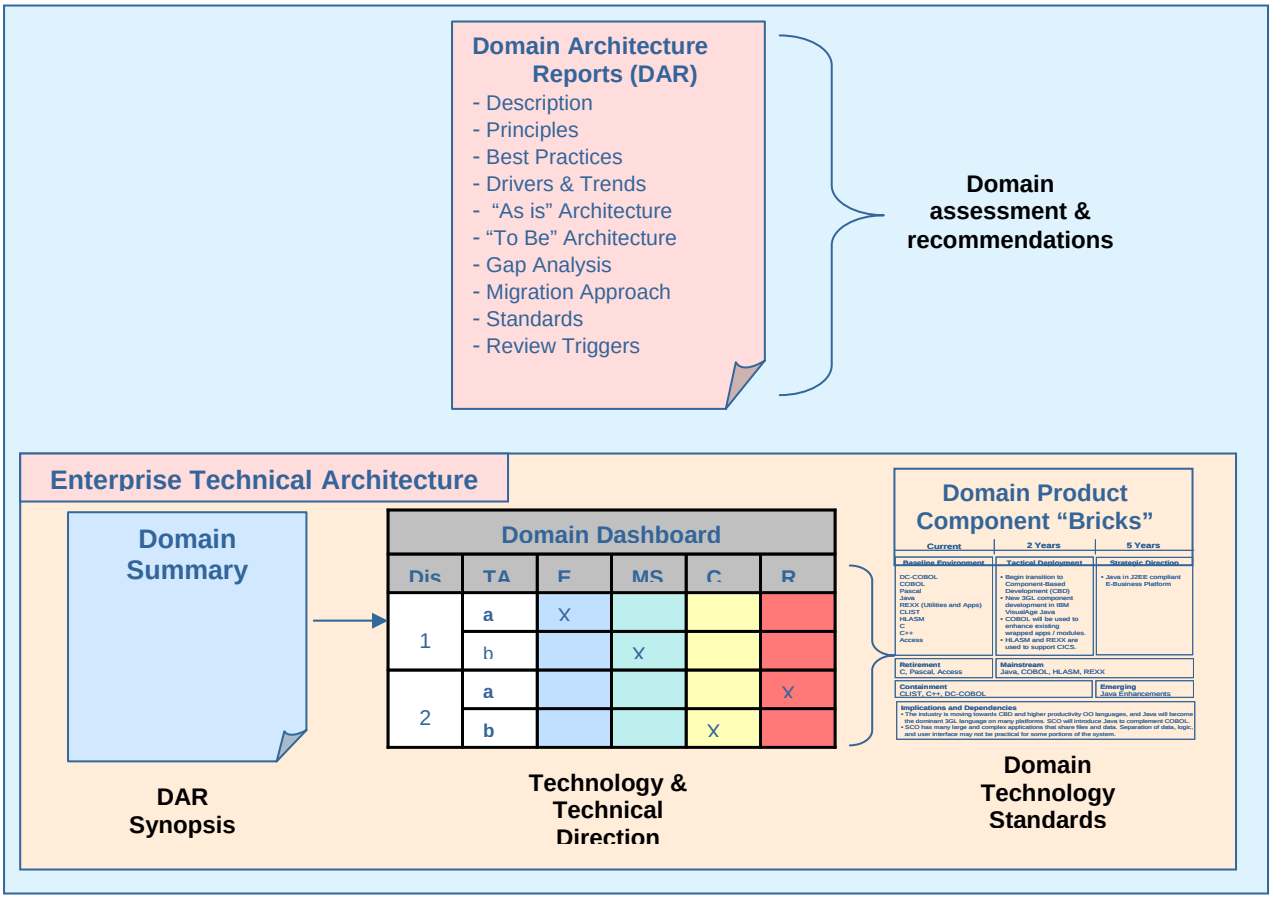

Figure 7 Domain Team Deliverables

Agency or departmental level domain teams use State level domain architecture reports, domain architectures, and the ETA development process to create an enterprise technical architecture that is germane

to their organization. This is accomplished by preparing domain summaries, domain dashboards, and creating a set of "bricks" about the technology products used within their organization. Product component "bricks" provide technical direction based on assessment of the technology's lifecycle, trends, and other key drivers. Based on this assessment, domain teams make decisions concerning standards for use and list them on the domain dashboard. Collectively product component "bricks" along with the domain dashboards and domain summaries become the organization's ETA.

The Domain Team Handbook contains a more detailed description of the ETA development process and provides a set of templates for use to document results.

5.2 ETA Governance

California utilizes a two tier governance approach one at the State level and one at an Agency/Department level to govern technology use. At the state level, governance focuses on establishing and maintaining the State's TAF and ETA standards. At the agency and department level, governance focuses on aligning Agency/Department ETA's with the State's "To be" technical architecture and establishing specific technical direction that moves their organization to the target architecture.

At the state-level, California's TA Framework and ETA are developed through a collaborative state-wide effort lead by the California Enterprise Architecture Program. The State's Technical Architecture Framework, Domain Team Handbook, and Domain Architecture documents are submitted to the State's Governance Organization (figure 8) for review and approval. The EA Committee along with the EA Committee conducts reviews and makes recommendations, to the IT Council who acts as the approval authority. CEAP facilitates the review process.

Note: *The State level governance is in a formative stage and may change from what is described above.*

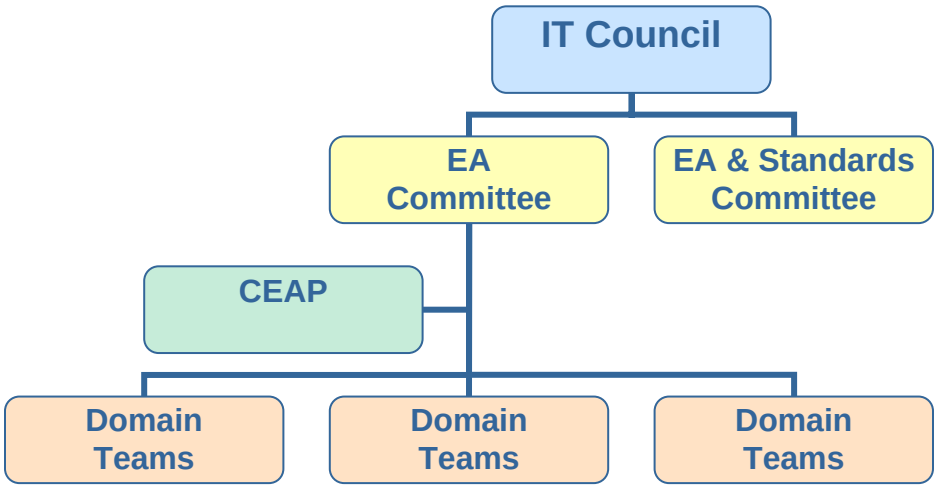

Figure 8 - ETA Governance Organization

5.2.1 IT Council Role

The IT Council advises the State Chief Information Office (CIO) concerning the efficient management and oversight of information technology used to support the operations of California's Executive Branch of

government. The Council makes recommendations to the State CIO on matters affecting information technology to include information technology standards and policies as applicable to the Executive Branch. Specifically the Council helps insure alignment of business activities and use of IT resources as appropriate in the context of agency and program initiatives and major service delivery requirements.

5.2.2 EA and Standards Committee Role

This committee reviews the TAF and ETA documentation provided by the EA Committee and makes appropriate policy recommendations to the IT Council concerning the use of the TAF, domain architecture reports, and technology standards.

5.2.3 EA Committee Role

The EA Committee provides guidance and direction to CEAP concerning development of the TAF and Domain Team handbook and regarding ETA development priorities. The committee charters Domain Teams that help create the State's ETA and reviews domain architecture reports and makes recommendations to the EA & Standards Committee and IT Council.

5.2.4 California Enterprise Architecture Program (CEAP) Role

CEAP is charged by the State CIO and the EA committees to develop and maintain the TAF and Domain Team Handbook. In doing so, CEAP collaborates with the State IT community to create these documents. CEAP also provides advice and assistance to Domain Teams and acts as liaison between the EA Committees and Domain Teams to facilitate domain architecture development and review activities. CEAP supports the EA Committee by reviewing Domain Architecture Reports and providing recommendations.

5.2.5 Domain Team Role

Domain teams are established for each technology domain (or in some cases disciplines) to develop ETA standards for the technologies included in their domain. Domain teams consist of subject matter experts (SME's) who are highly experienced with the technologies and knowledgeable of technology trends related to their domain. State level domain teams employ the TAF and processes included in the Domain Team Handbook to prepare domain architecture report, establish a state level domain architecture, and if need be update the domain TRM contained in the TAF. These teams also monitor technology triggers (identified in the architecture report), conduct periodic reviews, consider exception requests, and recommend changes to the architecture and technology standards established for their domain.

Note: The Domain Team Handbook contains detailed descriptions of responsibilities for domain team members.

5.2.6 Agency and Departmental Role

Agency and Department level governance helps insure alignment and consolidation of their technology based on the State's ETA and oversees the establishment of an ETA germane to their organization. Agencies/Department's determine additional technology standards and provide specific technical direction needed to implement migration to the State's target ("To be") architecture based on the drivers and constraints that affect their organizations.

5.3 ETA Processes

This section provides a general overview of the processes domain teams use to develop or review domain architectures. Detailed descriptions of each process can be found in the Domain Team Handbook.

5.3.1 Domain Architecture Development Process

The Domain Architecture Development Process is used to create technology domain architectures including standards. The process establishes a series of activities that domain teams use to research, assess, and create domain architecture reports. These reports include domain specific technology standards.

5.3.2 Standards Adoption/Exception Review Process

Once domain architectures are established to create the State's ETA, the ETA Standards Adoption/ Exception Review Process provides the mechanism to make decisions and control changes. Originators submit proposed changes or exception requests for consideration to the appropriate domain team. Requests are reviewed and analyzed to determine appropriateness in terms of strategic alignment, drivers, technology direction, and implications to the State's program initiatives. Findings and recommendations are provided for review and approval to the state's governance organization. Actions to update the ETA (i.e. domain architectures) are taken based on the decisions of the governance organization.

5.4 ETA Documentation

Domain architectures and standards are documented using the architecture report format and a series of ETA templates found in the Domain Team Handbook. Likewise other templates are provided that allow Agencies/Departments to request adoption of new standards or exceptions to existing technology standards.

Note: A set of templates used to document domain architecture are provided in the Domain Team Handbook.

5.4.1 Domain Architecture Reports (DAR)

The DAR is used to document the results of the Domain Team's development efforts. The report provides the following information about each domain and identifies the attachments that document the Domain architecture.

- Domain description
- IT Principles
- Domain best practices
- Business and technology drivers
- "As is" architecture
- "To be" architecture
- Gap Analysis
- Migration Strategy
- Review Triggers
- Technology Standards

Attachments:
- Domain Profile
- Domain Dashboard
- Product Component Summaries ("bricks").

5.4.2 Domain Profile

Domain Summaries provide a brief synopsis of the DAR to create a domain profile.

5.4.3 Domain Dashboard

The domain dashboard is used to list and relate the technologies found at each level within the domain i.e. disciplines, technology areas, and product components. The dash board also depicts the assessed status of the product components.

5.4.3 Technology Area/Product Component Summary ("Bricks")

These summaries document current and projected use of specific technology products or standards (e.g. application versions, hardware product, or industry standard). These summaries also known as "Bricks", are the lowest level at which technology within the domain architecture is managed and as such are the fundamental building blocks used for creating technical solutions for business. These templates convey the technology's lifecycle status (i.e. newly released product through retirement), technical direction, and provide guidance for usage (i.e. mainstream, contain, retire, etc.). Once populated, this template contains the technology standards associated with a product component.

These templates also provide technical direction by listing significant technology trends or planning/ programmatic dependencies that will cause specific product component technologies to move from one technology lifecycle phase to the next. Templates identify the opportunities that exist to either introduce new technologies or retire old ones and list the triggers that would necessitate a review of the "Brick" in order to determine if there is a need for change.

6.0 Developing an ETA

The TA Framework and Domain Team Handbook provide the approach, processes, and templates needed to create the State's ETA. State level domain teams use these documents to develop domain architectures. State level domain architectures are not only a component part of the State's ETA, but also provide an overall set of technology standards and broadly defined technical direction needed for guiding the State's use of technology.

6.1 Development Approaches

The "Just in Time" development approach and the "Programmed" development approach are the two primary alternatives recommended for use in developing an Enterprise Technical Architecture. These approaches depend on awareness of the business and technology issues and employ the ETA Development Process. Both approaches help identify the scope of each effort and promote incremental development.

6.1.1 "Just in Time" Development Approach

The "Just in Time" development approach develops and provisions the ETA based on the immediate needs of the enterprise. Typically this approach identifies the technologies needed to support urgent business requirements, address significant near term risk caused by IT obsolescence, or support current year programmatic actions (FSR's, BCP's, RFP's, etc.). The technologies associated with these needs are mapped to the TAF's TRM to determine which domains require development. Domain teams are established, and then tasked to implement development of all or selected portions of their domain architecture. This approach develops the ETA on an as needed basis rather than pursuing comprehensive, systematic development of all domains or technology areas at once. Therefore, the ETA is developed incrementally over time with those technology areas most needed to support the operational activities and program initiatives being developed first.

When the "Just in Time" development approach is used, Domain Teams need to make sure they are "Doing Just Enough" to provide a timely response to the need for architecture. This means that as domain teams develop the architecture, they do just enough "As is" and "To be" architecture, gap analysis, migration

planning, and standards development to add value when producing the Domain Architecture Report and the domain architecture.

6.1.2 Programmed Development Approach

The Programmed Development Approach is a prioritized, systematic effort that results in a fully developed ETA. This approach prioritizes and schedules development of all domains employing some of the same considerations used in the "Just in Time" Approach. The Programmed Approach incrementally develops the ETA by sequencing domain architecture development based on the organization's drivers and program initiatives. A fully developed ETA allows greater agility and rapid response to changing business activities, technology, and regulatory requirements.

6.2 State Level Implications

The implications of having a common TA Framework and State-level ETA are as follows.

- Projects the State as the enterprise
- Allows Control Agencies to use ETA information to evaluate proposed use of technology.
- Guides Agencies/Departments to a more common, modern technology architecture (i.e. "To be" architecture).
- Supports implementation of program initiatives identified by the State's IT Strategic Plan.
    - California Portal
    - Service Oriented Architecture (SOA)
    - GIS Program
    - Shared Services
    - IT Consolidation
- Provides information that allows Agencies/Departments to align and extend the ETA appropriately within their organization.

6.3 Agency/Departmental Implications

Agencies and Departmental implications include the following:

- Allows Agencies and Departments to align themselves within the context of the State as the enterprise.
- The State TA Framework provides a methodology for developing ETA at the Agency or Department level.
- The State's ETA allows Agencies and Departments to improve information sharing by aligning technologies with their business partners.
- Domain Architecture Reports provide information ("To be" architecture, technology trends, migration approaches, etc.) that facilitates development of Agency/Department specific migration steps.
- The State ETA allows Agencies and Departments to focus their ETA development efforts on defining their current technical environment, validating drivers, establishing germane technical direction, and identifying specific standards.
- The State level Technology Area/Product Component Templates ("bricks") identify the strategic direction and emerging technologies for Agency/Department Product Component Templates.
- Agencies can use the State's ETA to identify the technologies needed in support of FSR alternatives.

6.4 Benefits

Implementing the TA Framework and Domain Team Handbook affords numerous benefits at whatever level it is employed. By investing the time to use the framework to establish an ETA, the State and Agencies/Departments can more effectively manage technology, increase leverage of proposed technology investments, and reduce costs and risks associated with operating an IT infrastructure. Specifically, the State can expect to realize the following benefits from implementing the TAF and Domain Team Handbook:

- Provide a common understanding of how technology is organized and managed across the State
- Insure technical alignment within and across all levels of government (Federal, State, and Local) to increase interoperability and data sharing.
- Standardize and consolidate the State's use of information technology.
- Leverage IT investments appropriately across the State or Community of Interest.
- Rapidly respond to evolving business needs and technology drivers.
- Furnish technology standards and technical direction required for cost-effective management of the IT infrastructure.
- Help identify, control, and plan for necessary technology changes by:
    - Monitoring the lifecycle of existing technologies.
    - Determining retirement targets and planning for migration prior to obsolescence.
    - Identifying emerging technologies for future use within the enterprise.
- Support development of strategic plans and programs.
- Help expedite the acquisition of IT products/services.

7.0 Communicating the State's TRM Framework and ETA

Timely, effective communication concerning the development and use of the TA Framework, Domain Team Handbook, and ETA is critical. Without two-way communication few if any benefits can be realized. The CEAP insures adequate communication is provided to enable collaboration during development, furnish access to TAF and ETA information, and respond rapidly to Agency/Department requests. The CEAP website will be used to publish information about the TAF and the State's ETA. The website will also be used to provide access to a repository containing framework and ETA documentation.

8.0 Summary

The TA Framework is a part of California's Enterprise Architecture Program. It incorporates approaches and best practices obtained from the Federal Government, NASCIO, other State Agencies, and Gartner research. The framework provides an overall methodology for developing an Enterprise Technical Architecture (ETA). The methodology consists of a TRM, domain definitions, processes, and templates. The framework divides California's technical architecture into seven major areas of technology called domains and provides a domain specific TRM for each. The TRM establishes a hierarchy to group technologies within a domain into functionally based groupings called disciplines, technology areas, and Product Components.

Domain teams, comprised of subject matter experts representing multiple agencies and departments, collaborate to produce the State's ETA and technical standards. Teams use the Domain Architecture Development Process and technology templates found in the Domain Team Handbook to develop Domain Architecture Reports, Domain Summaries, Domain Dashboards, and Technology Area/Product Component Summaries ("bricks"). Creating this documentation for each domain populates California's ETA.

CEAP maintains the TAF document and the Domain Team Handbook. Domain Teams maintain the ETA by monitoring drivers and specific event triggers or responding to architectural change requests. These activities initiate a review process that determines if changes to the ETA are required. CEAP coordinates governance reviews in response to change or exception requests using the ETA Standards Adoption and

Exception Process. After collaboration and vetting with Agencies and Departments, the TAF, Domain Team Handbook, DAR's, and other outputs are submitted to the State IT Governance organization for approval. Once approved the TA framework and ETA documents are made available using the CEAP's website.

The TA Framework's methodology along with the State's ETA (i.e. Domain Architecture Reports, Domain Dashboards, and "Bricks") allows Agencies and Departments to develop an ETA for their organization. The State level ETA provides the information needed to establish a common target ("To be") architecture for each Agency and Department. The State's technical direction allows agencies or departments to select specific IT products based on an overall set of statewide standards. This allows for alignment of technology across the state, leveraged IT investments, improved data sharing and interoperability, and decreased IT infrastructure costs.

9.0 References

9.1 Documents

1. State of California, *California State Information Technology Strategic Plan*, November 2004

2. State of California, California Performance Review Report

3. Chief Information Officers Council, *Federal Enterprise Architecture Framework*, Version 1.1, September 1999

4. Chief Information Officers Council, *A Practical Guide to Federal Enterprise Architecture*, Version 1.0, February 2001

5. Federal Enterprise Architecture Program Management Office, *The Business Reference Model*, Version 2.0, June 2003

6. Federal Enterprise Architecture Program Management Office, *The Service Component Reference Model*, Version 1.0,

7. Federal Enterprise Architecture Program Management Office, *The Technical Reference Model*, Version 1.1, August 2003

8. Federal Enterprise Architecture Program Management Office, *The Data Reference Model*, Version 1.0, September 2004

9. National Association of State Chief Information Officers, *Enterprise Architecture Development Tool-Kit*, Version 3.0 October 2004

9.2 Web Sites

1. California State Chief Information Officer, California Information Technology Council, Committees http://www.cio.ca.gov/ITCouncil/Committees/ArchStandards.html .

2. Office of Management and Budget, Federal Enterprise Architecture, E-Gov, http://www.whitehouse.gov/omb/egov/a-1-fea.html .

3. NASCIO - NASCIO Enterprise Architecture Development Tool-Kit v3.0 http://www.nascio.org/publications/index.cfm .

4. Pennsylvania – EA Program http://www.oit.state.pa.us/eashare/site/default.asp?eashareNav=| .

5. Michigan – Technical Architecture http://www.michigan.gov/documents/Appendix_J_91642_7.pdf .

6. Virginia – Technical Architecture Library. http://www.vita.virginia.gov/cots/ea/library/index.cfm

7. South Carolina – Technical Architecture Taxonomy http://www.cio.sc.gov/SCEA/Taxonomy.pdf .

8. North Carolina - State Wide Technical Architecture http://www.ncsta.gov/.

9. Gartner Corporation – EA Research Articles www.gartner.com .

Appendix 1 – Domain Technical Reference Models